DIA/SYS-4
DoDIIS Security Update

TPOC CONFERENCE
BRIEFING

Introduction

- Ron Clift

Information Assurance Specialist, SAIC

Supporting DIA/SYS-4A.

- (202) 231-2175 DSN 428
- cnclira@dia.ic.gov, Ronald.Clift@dia.mil or Ronald.A.Clift@saic.com

TPOC Topics

- Security Testing - Lessons Learned
- Security - What's Going On?

Lessons Learned

- Security Pre-testing not being done;
- Defense-in-Depth;
  - Least Privilege not being applied
  - Ports/Services being left open, even when not being used
    - Creates a potential for exploitation
- Need better communication regarding PDRs and CDRs;
- Need all Beta I & II test reports forwarded to DIA/SYS-4 or a work an effort with the JITF VTF

Security Approvals

- 546 + IATT/IATO/ATO
  - A lot of work involved to get these out

Security Future

- Currently working on revisions to the DoDIIS C&A Guide, DIAM 50-4, and the JDCSISSS
- Creating a JWICS Security Classification Guide
- The DIA INFOSEC mailbox (INFOSEC@dia.ic.gov) should be used for questions
  - For a direct contact either email cnclira@dia.ic.gov or phone (202) 231-2175/DSN 428. If the question can't be answered immediately, it will be forwarded to the SYS-4 staff for coordination
- A DIA/SYS-4A system/project POC list will soon be published on the SYS-4 web page

Security Future, Cont'd

- Vulnerability Assessments
  - Incorporate into standard Security Testing
  - Already setting up at JITF
  - Message soon to be released to SCOs and CCs
  - More to come!!!

JDCSISSS Changes

- 1.5.10 (U) The Program Management Office (PMO)/Program Manager (PM)
- ·Appointing an Information System Security Engineer (ISSE)/System Design Security Officer (SDSO) in writing, to ensure system design is developed and implemented with required security features and safeguards; ensure enhancements to existing systems provide equal or improved security features and safeguards; consult with the appropriate certifying organization(s) as early as possible.
- ·Coordinate a C&A schedule with the DAA or DAA Rep.
- 2.3.2 (U) Design Phase
- The DAA/DAA Rep along with the data owner determines the Levels of Concern (LOC) for Confidentiality, Integrity and Availability based on the information characteristics determined in the Concepts Development Phase. The DAA/DAA Rep then determines the required Protection Level based on the need-to-know, formal access approval(s), and clearance level(s), if applicable, of system users as compared to the sensitivity, formal compartments, and classification of the data to be stored, processed, or transmitted on the system.

JDCSISSS Changes, Cont'd

2.3.2.2.2 (U) Security Documentation (SSP/SSAA) Requirements
The LOCs for Integrity and Availability and the PL for Confidentiality are identified using DCID 6/3 Chapters 4-6. During the design phase, the Project Management Office (PMO) ensures development of the Security Requirements Traceability Matrix (SRTM) and the continued development of the SSP/SSAA. This is a living document and should be updated throughout the.

2.3.4.1 (U) Time Line for Certification Activities
The timeline for certification activities will be coordinated with the certifying organization. A minimum 90-day period is the basis….

JDCSISSS Changes, Cont'd

4.3.3 (U) DoDIIS Certification and Accreditation for Exercise or Experiment Scenarios

The DoDIIS certification process for exercise/experiment will vary somewhat from the standard requirements. Lessening of the requirements for exercises/experiments is based time/risk limitations, on the limited duration and that consequences from any security incidents should be negligible, since most information being processed will be exercise traffic. Any approval or IATO is for the duration of the exercise/experiment only. An IATO is not to be construed as an automatic approval for future operational use, unless otherwise specified by approving authority. The criteria for determining which requirements apply are based on 1. No live connections; 2. JWICS live only; and 3. Live JWICS and other networks.

JDCSISSS Changes, Cont'd

4.3.3.1 (U) Simulated Network Connectivity

If the exercise/experiment architecture is using simulation network connectivity (i.e., simulated JWICS (SCI), SIPRNET (Secret), etc..), then the requirements will be as follows:

- SSAA (Abbreviated per SCO/Local ISSM)
- System Architecture/Diagrams
- Local ISSM review (Local ISSMs can review/approve PL2 exercise systems with SCO concurrence)
- SCO concurrence

4.3.3.2 (U) JWICS Connection

If JWICS only connection, above applies in addition to below:

- DIA Concurrence

4.3.3.3 (U) Exercise Use of Multiple Operational Network Connectivity

If the exercise/experiment will be using more than one operational/live network connections with limited duration, the following requirements apply:

- SSAA (SRTM, Test Procedures, TFM, etc. is abbreviated per SCO/DIA)
- System Architecture/Diagrams
- MOAs if interconnections
- SCO recommendation
- DAA concurrence/approval

JDCSISSS Changes, Cont'd

6.3.1 (U) Identification and Authentication Requirements

- Screen locks are mandatory, and require a password for reentry into the system. If an IS is idle for 15 minutes, the screen lock shall be activated automatically. Screen locks are not authorized in lieu of log-off procedures. Operations may require exceptions which must be approved by the ISSPM/SCO.

6.3.2 (U) Password Requirements

- Password evaluation tools may be used by sites for security assessment. Approval must be obtained through the ISSM.

Conclusion

- Questions??????????